Jurnal Sarjana Teknik Informatika
Volume 2 Nomor 2, Juni 2014
e-ISSN: 2338-5197

VISUALISASI ALGORITMA *CHIPER BLOCK CHAINING* SEBAGAI MEDIA PEMBELAJARAN BERBASIS *MOBILE* ANDROID

[1]Muhamad Rijal Faqih, [2]Eko Aribowo (0006027001)

[1,2]Program Studi Teknik Infromatika
Universitas Ahmad Dahlan
Prof.Dr.Soepomo,S.H.,Janturan,Umbulharjo,Yogyakarta 55164
[1]Email: farizaldo@yahoo.co.id
[2]Email: koab@tif.uad.ac.id

ABSTRAK

Kriptografi merupakan salah satu materi utama dalam mata kuliah keamanan komputer. Mata kuliah keamanan komputer merupakan salah satu mata kuliah wajib di program studi teknik informatika, Universitas Ahmad Dahlan, Yogyakarta. Waktu pertemuan dalam perkuliahan keamanan komputer sesuai dengan satuan perkuliahan (SAP) hanya 14 kali pertemuan. Metode-metode kriptografi yang dibahas sangat banyak, diantaranya metode Chiper Block Chaining. Pembahasan Metode kriptografi ini tidak dibahas secara mendetail hanya dibahas 1 kali pertemuan saja. Jadi tidak memungkinkan mahasiswa mampu memahami tentang algoritma metode kriptografi tersebut secara mendetail di kelas.

Subjek peneltian ini adalah merancang suatu proses visualisasi proses enkripsi dan dekripsi untuk mendukung proses pembelajaran kriptografi, metode yang digunakan dalam proses enkripsi dan dekripsi adalah metode Chiper Block Chaining. Langkah pengembangan aplikasi diawali dengan pengumpulan data dari banyaknya mahasiswa yang menggunakan smartphone berbasis android dilanjutkan dengan studi pustaka dan mengamati program-program kriptografi. Merancang tampilan aplikasi dan mengimplementasikan hasil rancangan menjadi sebuah program. Melakukan pengujian program dengan blackbox test dan alpha test.

Dalam penelitian yang dilakukan dihasilkan sebuah perangkat lunak visualisasi Chiper Block Chaining yang dikemas dalam bentuk aplikasi yang berbasis android, program enkripsi dan dekripsi karakter teks menggunakan bahasa pemrograman android yang berbasis java, hasil ujicoba yang telah dilakukan menunjukan bahwa aplikasi ini sudah layak dan dapat dimanfaatkan.

Kata kunci : *Security Computer, Kriptografi, Chiper Block Chining, Android, Visualisasi*

 e-ISSN: 2338-5197

1. PENDAHULUAN

Cipher Block Chaining adalah salah satu pengembangan dari algoritma Block cipher, algoritma ini akan membagi-bagi teks terang yang akan dikirimkan dengan ukuran tertentu (disebut blok) dengan panjang bit tiap blok sesuai dengan panjang bit pada kunci, dan setiap blok dienkripsi dengan menggunakan kunci yang sama dan di XOR-kan dengan hasil enkripsi blok sebelumnya, untuk enkripsi blok pertama menggunakan inisialition vektor atau biasa disebut IV atau C0 sebagai pengganti dari hasil enkripsi blok sebelumnya.[3]. Materi algoritma ini di perkuliahan diajarkan hanya satu kali pertemuan, dengan keterbatasan waktu tersebut maka materi yang diajarkan tidak terlalu mendetail, maka diperlukan materi di luar jam perkuliahan, salah satu caranya adalah dengan membuat suatu aplikasi media pembelajaran yang melingkupi isi materi ditambahkan dengan simulasi berupa sebuah animasi sehingga mahasiswa bisa mengetahui secara detail dari proses kriptografi yang sedang terjadi dan mempermudah mahasiswa dalam mempelajari materi kriptografi algoritma *Chiper Block Chaining*.(Prana Andypal, 2011)

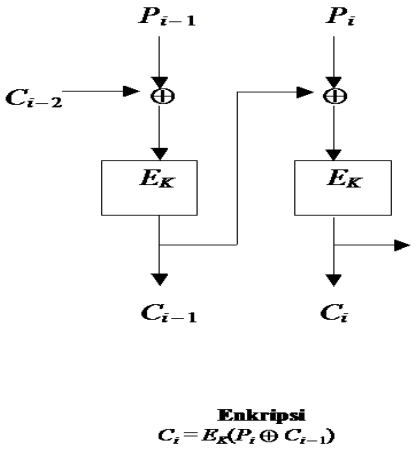
2. KAJIAN PUSTAKA

Ilmu kriptografi adalah ilmu yang mempelajari tentang penyembunyian huruf atau tulisan sehingga membuat tulisan tersebut tidak dapat dibaca oleh orang yang tidak berkepentingan.. Kriptografi mempunyai 2 (dua) bagian yang penting, yaitu *enkripsi* dan *dekripsi*. *Enkripsi* adalah proses dari penyandian pesan asli menjadi pesan yang tidak dapat diartikan seperti aslinya. *Dekripsi* adalah merubah pesan yang sudah disandikan menjadi pesan aslinya. Pesan asli biasanya disebut *plaintext*, sedangkan pesan yang sudah disandikan disebut *ciphertext*.(Rinaldi Munir, 2006)

2.1 Algoritma *Cipher Block Chaining*

Salah satu alternatif untuk mencegah munculnya blok-blok *ciphertext* yang sama dari blok *plaintext* yang sama pada satu pesan adalah dengan menggunakan mode CBC. Pada skema ini setiap blok n-bit *plaintext* di-XOR-kan dengan blok n-bit *ciphertext* sebelumnya. Kecuali blok *plaintext* pertama di-XOR-kan dengan suatu konstanta awal atau initialization vector (IV), sebesar n-bit. Hasil dari proses XOR tersebut yang kemudian di*enkripsi*.[2]

Gambaran skema *enkripsi* CBC dapat dilihat pada gambar 1 di bawah ini:



Gambar 1. Skema *Enkripsi* CBC

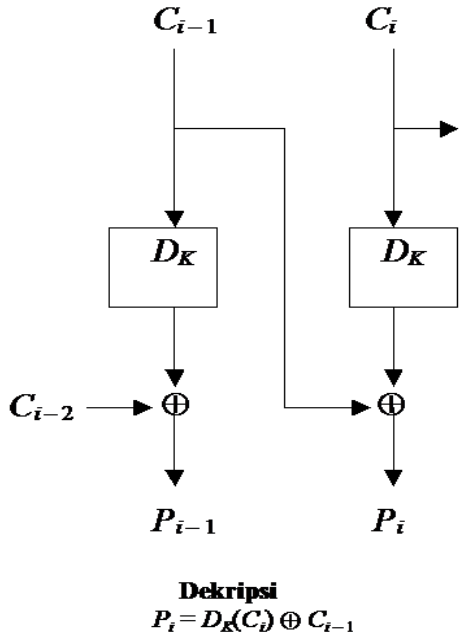
Untuk proses *dekripsi*, hasil *dekripsi* blok *ciphertext* di-XOR-kan dengan blok *ciphertext* sebelumnya untuk menghasilkan blok *plaintext*. Untuk blok pertama, hasil *dekripsi* blok *ciphertext* pertama di-XOR-kan dengan IV

 e-ISSN: 2338-5197

untuk menghasilkan blok *plaintext* pertama. Walaupun nilai IV tidak perlu dirahasiakan akan tetapi integritas dari nilai IV harus dilindungi. [2]

Gambaran skema *dekripsi* CBC dapat dilihat pada gambar 2 di bawah ini.

Perhatikan kelemahan yang dimiliki metode ini yaitu kesalahan satu bit pada sebuah blok *plaintext* akan merambat pada blok *ciphertext* yang berkoresponden dan semua blok *ciphertext* berikutnya, mode CBC juga memiliki Keuntungan yaitu karena blok-blok *plaintext* yang sama tidak menghasilkan blok-blok *ciphertext* yang sama, maka kriptanalisis menjadi lebih sulit, Inilah alasan utama penggunaan mode CBC digunakan.



Gambar 2. Skema *Dekripsi* CBC

Secara matematis, *enkripsi* dengan mode CBC dinyatakan sebagai $C_i = E_K(P_i \oplus C_i - 1)$ dan *dekripsi* sebagai $P_i = D_K(C_i) \oplus C_i - 1$

Blok *plaintext* pertama menggunakan C_0 sebagai vector awal (initialization vector atau IV). IV tidak perlu rahasia.Blok-blok *plaintext* yang identik di*enkripsi* menjadi blok-blok *ciphertext* yang berbeda hanya jika blok-blok *plaintext*nya sebelumnya berbeda.(Heru Kurniawan, 2013)

2.2 Android

Android adalah sistem operasi yang berbasis Linux untuk telepon seluler seperti telepon pintar dan komputer tablet. Android menyediakan platform terbuka bagi para pengembang untuk menciptakan aplikasi mereka sendiri untuk digunakan oleh bermacam piranti bergerak.

Sebagai sebuah sistem operasi terbuka yang dikembangkan oleh sebuah konsorsium yang besar, perkembangan Android sangat pesat. Hingga saat ini Android telah memiliki beberapa versi sebagai pengembangan dari versi sebelumnya.(Wikipedia, 2009)

3. METODOLOGI PENELITIAN

Subjek penelitian yang akan dibahas pada tugas akhir ini adalah bagaimana membangun aplikasi visualisasi algoritma *Cipher Block Chaining* berbasis mobile android dalam bahasa pemrograman android yang berbasiskan java. Analisis kebutuhan digunakan untuk memahami sistem yang akan dibangun. Pada tahap analisis digunakan untuk menentukan klasifikasi data yang tepat untuk mendukung pembuatan rancangan aplikasi data yang lebih mudah diakses dengan program aplikasi yang digunakan sebelum tahap perancangan menu tampilan untuk aplikasi visualisasi algoritma *Cipher Block Chaining* berbasis mobile android,

 e-ISSN: 2338-5197

terlebih dahulu dilakukan analisis data dengan menganalisis seberapa sistem yang akan dibuat mampu menyelesaikan masalah terutama dalam hal memberikan kemudahan user dalam melakukan visualisasi pembelajaran.

4. HASIL DAN PEMBAHASAN

4.1 Analisis kebutuhan system

Dari penelitian ini, dapat dihasilkan sebuah program aplikasi yaitu visualisasi proses *enkripsi* dan *dekripsi* metode *Cipher Block Chaining* pada perangkat mobile berbasis android untuk mendukung proses pembelajaran kriptografi Hasil dari penelitian akan menghasilkan sebuah program aplikasi yang:

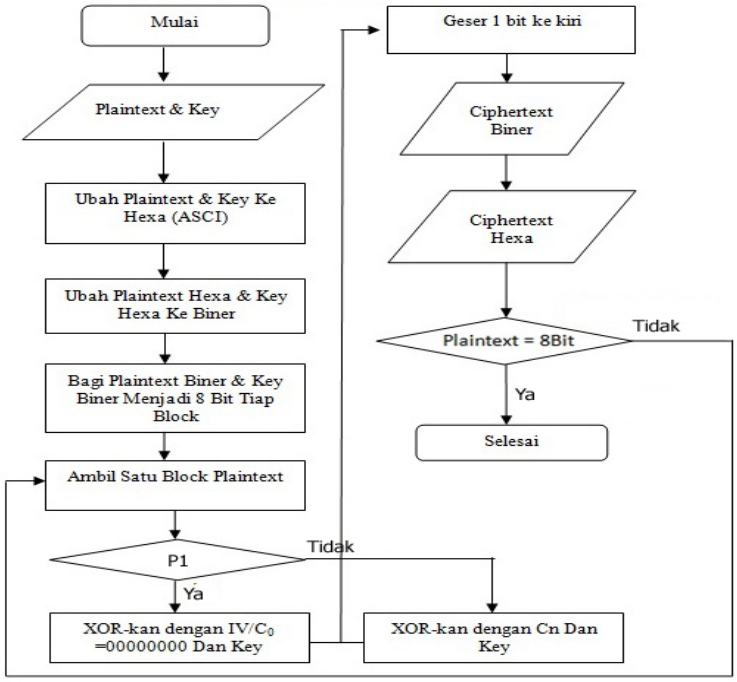
1. Dapat melakukan proses enkripsi, yaitu proses mengubah karakter berita atau plaintext menjadi karakter yang terenkripsi atau chipertex dengan menambahkan kunci/key yang telah ditentukan.
2. Dapat melakukan proses dekripsi, yaitu proses pengembalian karakter yang telah terenkripsi atau chipertext menjadi karakter berita atau plaintext dengan memasukan karakter kunci/key yang telah ditentukan
3. Memberikan suatu contoh proses visualisasi enkripsi dan dekripsi metode Cipher Block Chaining yang dikemas dalam media mobile berbasis android.

4.2 Perancangan SISTEM

Perancangan visualisasi metode *Cipher Block Chaining* ini digambarkan dalam bentuk flowchart.

a. Flowchart *Enkripsi Cipher Block Chaining*

Perancangan diagram flowchart untuk proses *enkripsi Cipher Block Chaining* tampak seperti pada gambar 3 berikut

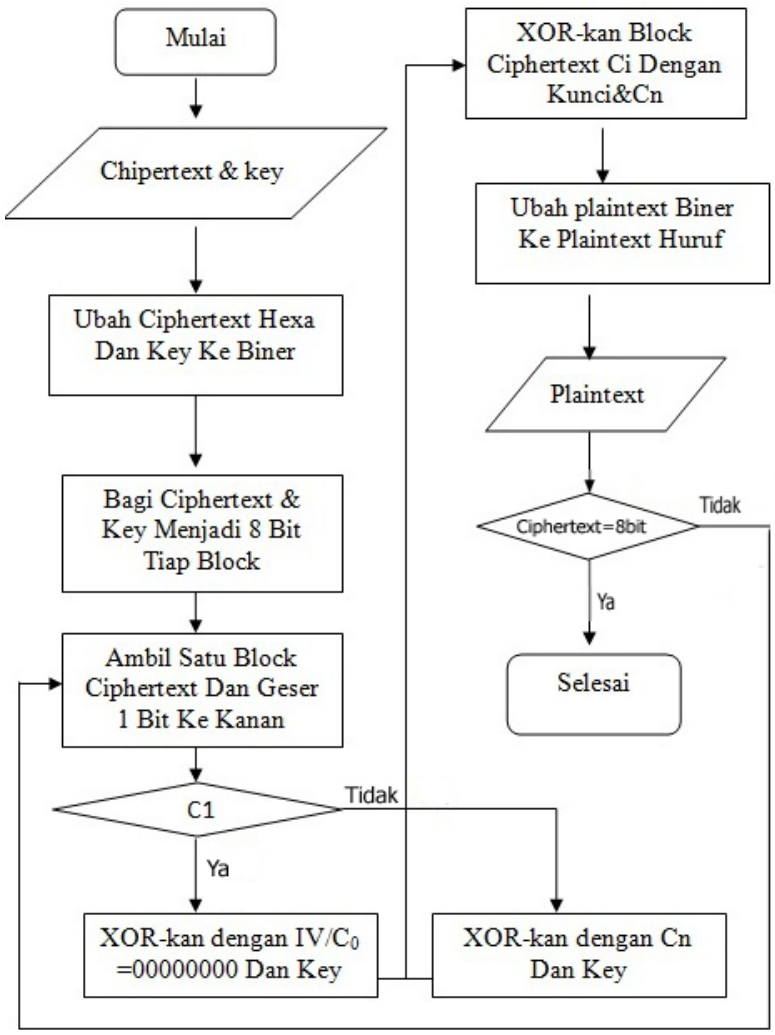


Gambar 3. Flowchart *Enkripsi* CBC

 e-ISSN: 2338-5197

b. Flowchart *Dekripsi ChiperBlock Chaining*

Perancangan diagram flowchart untuk proses *dekripsi Cipher Block Chaining* tampak seperti pada gambar 4 berikut ini



Gambar 4. Flowchart *Dekripsi* CBC

4.3 Implementasi

a. Halaman Utama

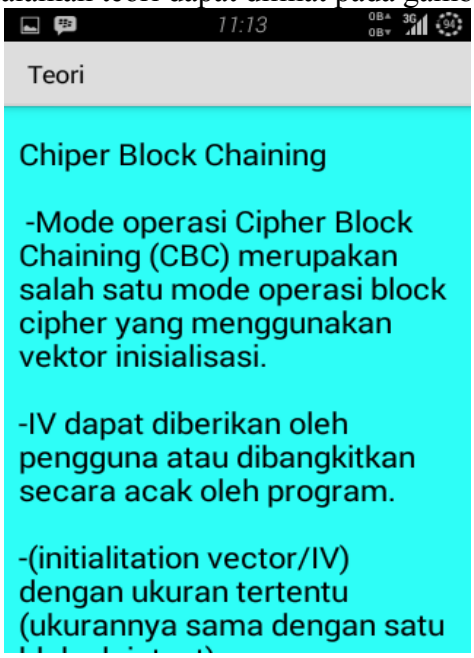
Halaman utama adalah halaman pertama kali ketika user membuka aplikasi visualisasi algoritma *chiper block chaining*. Halaman utama terdiri dari lima menu, lima menu itu adalah: menu teori, menu program, menu visualisasi, menu profil dan menu keluar dari aplikasi. tampilan halaman utama visualisasi dapat dilihat pada gambar 5 berikut ini:

 e-ISSN: 2338-5197

Gambar 5. Halaman Utama

b. Halaman Teori

Halaman teori berisi tentang teori-teori dari materi algoritma *Cipher Block Chaining*. Halaman teori dapat dilihat pada gambar 6



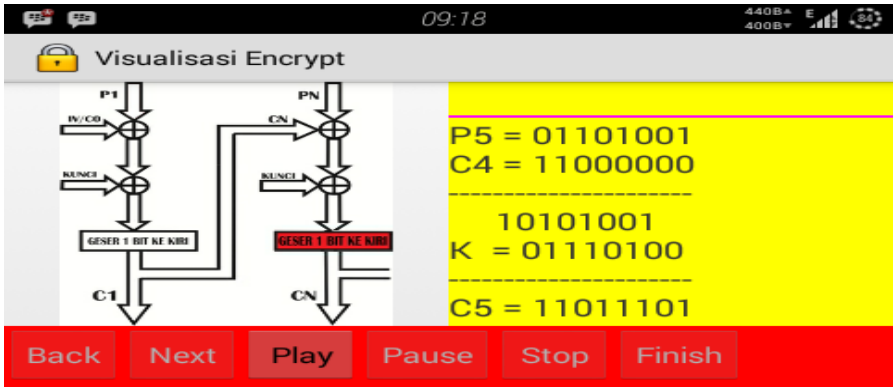
Gambar 6. Halaman Teori

c. Halaman Visualisasi

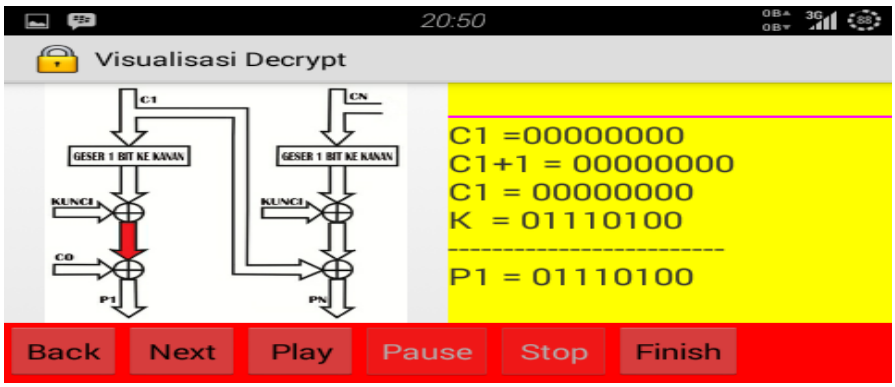
Halaman visualisasi adalah halaman yang berisi visualisasi dari program *enkripsi* dan *dekripsi*, dimana di halaman tersebut ditampilkan sebuah form yang diisi *plaintext/ciphertext*, kunci dan sebuah tombol *enkrip/dekrip* yang jika ditekan tombolnya akan menuju sebuah tampilan visualisasi yang menampilkan alur proses *enkripsi* atau *dekripsi* metode

 e-ISSN: 2338-5197

Cipher Block Chaining berupa teks dan gambar yang bergerak untuk menambah pemahaman materi yang ada. Menu halaman visualisasi dapat dilihat pada gambar 7, 8, 9, 10 dibawah ini.



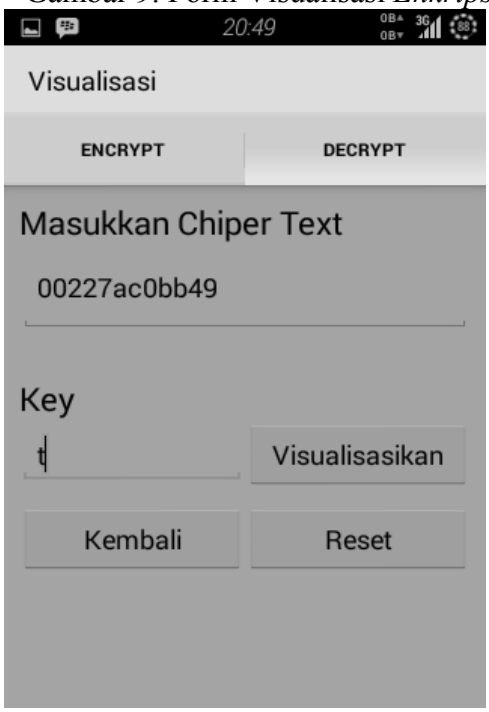
Gambar 7 Halaman Proses Visualisasi *Enkripsi*



Gambar 8 Halaman Proses Visualisasi *Dekripsi*

 e-ISSN: 2338-5197

Gambar 9. Form Visualisasi *Enkripsi*



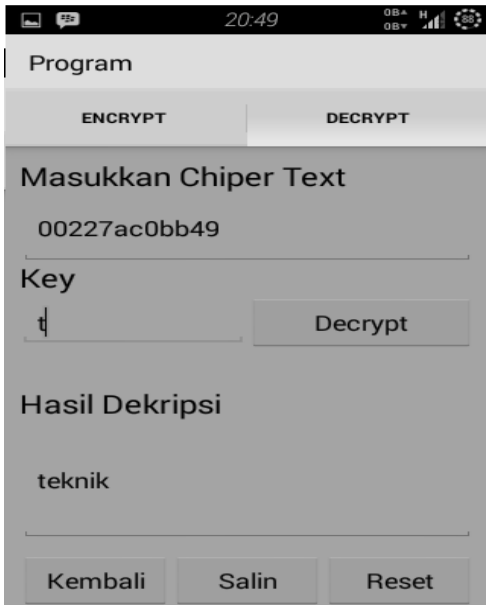
Gambar 10. Form Visualisasi *Dekripsi*

d. Halaman Program

Halaman program adalah halaman yang berisi menu untuk meng*enkripsi* dan *dekripsi* kata yang langsung diketahui hasilnya tanpa proses visualisasi, halaman program dapat dilihat pada gambar 11 dan 12 di bawah ini:

Gambar 11. Halaman Program *Enkripsi*

 e-ISSN: 2338-5197



Gambar 12. Halaman Program *Dekripsi*

4.4 Pengujian

Pengujian sistem adalah proses uji pada pembuatan sistem secara keseluruhan. Metode yang dilakukan dalam pengujian ini adalah *blackox test* dan *alpha test*. Pengujian sistem dengan *blackbox test* yaitu mengamati kinerja aplikasi yang telah dibuat. Pengujian sistem dilakukan dengan memberikan quisoner kepada dosen pengampu mata kuliah kriptografi, dosen penguji 1 dan mahasiswa yang mengambil tugas akhir denga topik algoritma *cipher block chaining*. Pertanyaan quisoner disesuaikan dengan analisis kebutuhan sistem. Pengujian sistem dengan *alpha test* yaitu pengujian yang dilakukan dengan cara meminta beberapa responden untuk mencoba aplikasi yang telah dibuat dan kemudian masing – masing akan diberikan sebuah quisioner yang digunakan untuk memberikan penilain, pengujian ini dilakukan dengan mengundang beberapa user mahasiswa yang telah mengambil mata kuliah keamanan komputer dan mata kuliah kriptografi untuk menguji coba aplikasi dan masing-masing user diberi daftar pertanyaan untuk memberikan pendapat tentang program yang dijalankan tersebut.

5. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan, dapat disimpulkan beberapa hal sebagai berikut:

1. Telah dihasilkan suatu aplikasi visualisasi metode *Chiper Block Chaining* yang dikemas dalam media mobile berbasis android.
2. Implementasi program ini menghasilkan suatu aplikasi yang dapat menguba *plaintext* yang berupa karakter-karakter teks menjadi kode-kode yang tidak dikenal (*chipertext*) menjadi teks aslinya(*plaintext*).
3. Aplikasi yang dihasilkan ini dapat digunakan untuk mengenkripsi dan mendekripsikan karakter-karakter teks yang terdiri dari huruf besar, huruf kecil, simbol, dan angka.

 e-ISSN: 2338-5197

4. Keuntungan mode CBC adalah karena blok-blok *plaintext* yang sama tidak menghasilkan blok-blok *ciphertext* yang sama, maka kriptanalis menjadi sulit mendekripnya.
5. Kelemahan dari aplikasi ini adalah apabila dijalankan pada *device* yang layarnya berukuran kecil maka tampilan tidak akan terlihat jelas, untuk mengatasinya maka dibutuhkan *device* yang layarnya berukuran besar.
6. Kelebihan dari aplikasi ini adalah aplikasi dapat dibuka kapanpun dan dimanapun karena sifatnya yang portable.

DAFTAR PUSTAKA

Andypal, Prana, 2011, "Simulasi Proses Enkripsi Dan Dekripsi Algoritma Rijndael Untuk Mendukung Proses Pembelajaran Kriptografi Berbais Web", Teknik Informatika Universitas Ahmad Dahlan.

Kurniawan, Heru, 2013, "Visualisasi Proses Enkripsi Dan Dekripsi Metode AADFGVX PRODUCT CHIPER DAN CHIPER BLOCK CHAINING", Teknik Informatika Universitas Ahmad Dahlan.

Munir, Rinaldi, 2006, "Kriptografi", Informatika, Bandung.

Wikipedia, 2005, "Multimedia", http://id.wikipedia.org/wiki/Multimedia. 17 Desember 2013.

Wikipedia, 2009, "Android (sistem operasi)", http://id.wikipedia.org/wiki/Android. 17 Oktober 2013.

Yuliana, Rahmawati, 2008, "Visualisasi alat bantu pembelajaran kriptgrafi asimetris RSA (Rishet Shamir Adleman)", Teknik Informatika Universitas Ahmad Dahlan.